



February 7, 2022

Re: S.B. 335 - Biometric Identifiers and Biometric Information Privacy

Dear Honorable Members of the Senate Finance Committee,

I write today on behalf of the Electronic Frontier Foundation, a non-profit organization that works to protect civil liberties in the digital age. EFF represents more than 35,000 active donors and members, including many in Maryland. We are writing to ask you to advance S.B. 335, Senator Feldman’s bill regarding Biometric Identifiers and Biometric Information Privacy.

It is critically important that lawmakers stand up to protect their constituents from the abuse of biometric information, through strong laws with strong enforcement. Biometric information is unique in many ways. For one, our biometrics are easy to capture. Once captured, we generally cannot change our biometrics, unlike our credit card numbers, or even our names. Databases of biometric information are [ripe targets for data thieves](#). That’s why EFF has worked to defend and enforce the Illinois Biometric Information Privacy Act (BIPA)—on which S.B. 335 is based—as a necessary means to protect our biometric privacy from intrusion by private entities. It is also why we have encouraged other states and the federal government to follow this model of legislation.

Since it was passed in 2008, Illinois’ BIPA has prevented one of the worst corporate uses of face recognition: dragnet faceprinting of the public at large. Some companies do this to all people entering a store, or all people appearing in photos on social media. This practice violates BIPA because some of these people have not previously consented to faceprinting.

We are encouraged to see Maryland recognize the harms that overbroad collection can inflict on people as they go about their daily lives. And we strongly encourage you not to weaken SB 335 by eliminating perhaps the most important piece of Illinois’ BIPA: the private right of action.

Laws are often only as good as their penalties. This is why it is a top priority for the Electronic Frontier Foundation to include private rights of action in privacy laws, including those that protect biometric privacy. Consumer enforcement is part of EFF’s “bottom-up” approach to public policy. Ordinary technology users should have the power to decide for themselves whether to bring a lawsuit to enforce their statutory privacy rights.

Since Illinois’ BIPA was passed in 2008, those seeking to weaken its protections have repeatedly attacked the private right of action, calling it unnecessary. Including a private right of action, in fact, is how legislators normally approach privacy laws. Many privacy statutes contain a private right of action, including federal laws on [wiretaps](#), [stored electronic communications](#), [video rentals](#), [driver’s licenses](#), [credit reporting](#), and [cable](#)

EFF letter re: S.B. 335
February 7, 2022
Page 2 of 2

[subscriptions](#). So do many other kinds of laws that protect the public, including federal laws on [clean water](#), [employment discrimination](#), and [access to public records](#).

We have already seen how ineffective laws become when they are passed without this important enforcement mechanism. Texas, for example, has a [2009 law very similar to Illinois' BIPA](#) except for the fact that only the state attorney general has the right to sue under the law. As a result, it has never been enforced.

Laws like BIPA that allow private citizens to sue are necessary for several reasons. First, biometric surveillance is a growing menace to our privacy. Our biometric information can be harvested at a distance and without our knowledge, and we often have no ability as individuals to effectively shield ourselves from this grave privacy intrusion. Second, BIPA follows in the footsteps of a host of other privacy laws that prohibit the capture of private information absent informed opt-in consent, and that define data capture without notice and consent as an injury in and of itself. Third, allowing private lawsuits is a necessary means to ensure effective enforcement of privacy laws.

Illinois' BIPA has been on the books for fourteen years and has proven itself one of the most effective laws at holding companies accountable for privacy violations in the country. For example, in 2021, Facebook settled a lawsuit with its Illinois users for [\\$650 million](#) after it collected faceprints from its users without their consent in violation of [BIPA](#).

People should be able to choose which companies they trust with their information, especially information as sensitive and unique as biometrics. Companies, no matter their size, should recognize the responsibilities inherent to the collection of biometric information. They also must be held accountable for actions that break that trust.

We thank you for considering this important issue, and we thank Senator Feldman for his leadership on this issue. If you have any further questions, please reach out to me, legislative activist Hayley Tsukayama, at hayleyt@eff.org. Thank you.

Sincerely,



Hayley Tsukayama
Legislative Activist
Electronic Frontier Foundation
(415) 436-9333 x 161